REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1, 4, 6, 22, 39, and 45 are amended. Claims 2, 3, 5, 42, and 48 are canceled without prejudice. Claims 1, 4, 6-41, and 43-47 are pending in this application.

35 U.S.C. § 102

Claim 1 stands rejected under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,047,325 to Jain et al. (hereinafter "Jain"). Applicant respectfully submits that claim 1 is not anticipated by Jain.

Jain is directed to network devices for implementing virtual local area networks and virtual private networks (see, col. 1, lines 11-13). As discussed in the Abstract of Jain, a network device implements a virtual LAN over interconnected computer networks transparent to the computer networks. Using authentication and encryption, a secure connection between network devices over a public wide area network implements a virtual private network and enables the definition of virtual LANs over the virtual private network.

In contrast, amended claim 1 recites:

> A computing device comprising:
> a set of filters;
> a mapping of virtual addresses to network addresses; and
> a controller, coupled to the set of filters and the mapping, to,
> access, upon receipt of a data packet requested to be sent from the computing device to a target device via a network, the set of filters and determine whether the data packet can be sent to the target device based on whether the computing device is allowed to communicate with the target device,

> replace, based on the mapping, the target address in the data packet with a corresponding target network address;
>
> forward the data packet to the target device at the target network address if it is determined the data packet can be sent to the target device; and
>
> prevent the computing device from modifying any of the filters in the set of filters, but allow the set of filters to be modified by a plurality of remote devices operating at a plurality of different managerial levels.

Applicant respectfully submits that no such system is disclosed in Jain.

Applicant respectfully submits that there is no discussion or mention in Jain to prevent the computing device from modifying any of the filters in the set of filters, but allow the set of filters to be modified by a plurality of remote devices operating at a plurality of different managerial levels as recited in amended claim 1. Although Jain discusses a filter table 74 (see, Fig. 4 and col. 4, lines 1-33), there is no discussion or mention in Jain that a computing device that comprises a set of filters, a mapping, and a controller as recited in amended claim 1 is prevented from modifying any filters, but a plurality of remote devices operating at a plurality of different managerial levels is allowed to modify the set of filters.

Additionally, Applicant notes that in the rejection of claim 2 in the March 28, 2005 Office Action at ¶ 7, p. 3, Audebert at col. 6, lines 46-61 and col. 12, lines 5-16 is cited as disclosing preventing unauthorized modification to the filter program. Audebert is directed to a terminal and system for performing secure electronic transactions (see, Title). As discussed in the Abstract of Audebert, the terminal includes a terminal module and a personal security device. The terminal module is adapted to receive high-level requests from an application (Fap) installed on an electronic unit. The high-level requests are independent of the

personal security device. There terminal module and/or the personal security device includes a reprogrammable memory for storing and a unit for executing a filter program translating the high-level requests into at least one of either (i) at least one sequence of exchanges of data between the terminal module and the user or (ii) a sequence of at least one elementary command that can be executed by the personal security device, together with a unit for protecting the filter program to prevent any modification of the filter program by an unauthorized entity.

The cited portions of Audebert discuss protecting filter software to prevent an unauthorized person reading and/or modifying the software, and preventing a pirate from using an integrated circuit card of a user without their knowledge. However, there is no discussion or mention that this unauthorized person or pirate is the computing device that comprises a set of filters, a mapping, and a controller as recited in amended claim 1, and that that computing device is prevented from modifying any filters, but that the set of filters is allowed to be modified by a plurality of remote devices operating at a plurality of different managerial levels.

Furthermore, Applicant notes that in the rejection of claim 5 in the March 28, 2005 Office Action at ¶ 12, pp. 4-5, Coss at col. 9, lines 7-18 is cited as disclosing remote proxy or administrator load filters. Coss is directed to methods and apparatus for a computer network firewall with stateful packet filtering (see, Title). As discussed in the Abstract of Coss, a firewall can support multiple security policies, multiple users or both, by applying any one of several distinct sets of access rules. Dynamic rules may be used in addition to pre-loaded access rules in order to simplify rule processing. To unburden the firewall of application

proxies, the firewall can be enabled to redirect a network session to a separate server for processing.

The cited portion of Coss discusses that dynamic rules can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions. However, Applicant respectfully submits that there is no discussion or mention in Coss that the computing device that comprises a set of filters, a mapping, and a controller as recited in amended claim 1 is prevented from modifying any filters, but that the set of filters is allowed to be modified by a plurality of remote devices operating at a plurality of different managerial levels.

For at least these reasons, Applicant respectfully submits that amended claim 1 is allowable over Jain.

Applicant respectfully requests that the §102 rejections be withdrawn.

35 U.S.C. § 103

Claims 2 and 3 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of U.S. Patent No. 6,694,436 to Audebert (hereinafter "Audebert"). Claims 2 and 3 have been canceled without prejudice, thereby rendering the rejection of claims 2 and 3 moot.

Claims 4, 39, 44, and 45 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of U.S. Patent No. 6,717,949 to Boden et al. (hereinafter "Boden"). Applicant respectfully submits that claims 4, 39, 44, and 45 are not obvious over Jain in view of Boden.

Boden is directed to selective masquerading of internal IP addresses among a plurality of public IP address (see, col. 1, lines 25-28). As discussed in the Abstract of Boden, a type of NAT (Network Address Translation), called masquerade NAT, defines a many-to-one mapping in such a way as to allow the 'many' to specify subsets of IP addresses. This allows traffic separation, which improves throughput to and from external networks (e.g., the Internet), and also improves flexibility in IP address management.

With respect to claim 4, claim 4 depends from amended claim 1 and Applicant respectfully submits that claim 4 is allowable over Jain for at least the reasons discussed above with respect to amended claim 1. Boden is not cited as curing, and does not cure, the deficiencies of Jain discussed above with respect to amended claim 1. Accordingly, for at least these reasons, Applicant respectfully submits that claim 4 is allowable over Jain in view of Boden.

With respect to amended claim 39, amended claim 39 recites:

> A method comprising:
> maintaining an association of virtual addresses and corresponding network addresses;
> making a computing device aware of the virtual addresses;
> hiding the network addresses from the computing device;
> receiving, from the computing device, a data packet intended for a target computing device corresponding to a target virtual address;
> replacing, based on the target virtual address, the target virtual address with the corresponding target network address;
> forwarding the data packet to the target computing device at the target network address;
> maintaining, at the computing device, a set of filters that further restrict the ability of the computing device to communicate with other computing devices;
> allowing the set of filters to be modified from a remote device; and

preventing the computing device from modifying the set of filters.

Applicant respectfully submits that no such method is disclosed or suggested by Jain in view of Boden.

Jain, as discussed above, is directed to network devices for implementing virtual local area networks and virtual private networks. Boden, as discussed above, is directed to selective masquerading of internal IP addresses among a plurality of public IP address. However, nowhere in either Jain or Boden is there any discussion or suggestion of maintaining a set of filters that further restrict the ability of the computing device to communicate with other computing devices, allowing the set of filters to be modified from a remote device, and preventing the computing device from modifying the set of filters as recited in amended claim 39.

Additionally, Applicant notes that in the rejection of claim 42 in the March 28, 2005 Office Action at ¶ 42, pp. 14-15, Audebert at col. 6, lines 46-61 and col. 12, lines 5-16 is cited as disclosing preventing unauthorized modification to filter software. These cited portions of Audebert discuss protecting filter software to prevent an unauthorized person reading and/or modifying the software, and preventing a pirate from using an integrated circuit card of a user without their knowledge. However, there is no discussion or mention that this unauthorized person or pirate is the computing device at which the set of filters is maintained, but that this unauthorized person or pirate is not a remote device. Furthermore, this prevention in Audebert is directed to particular persons, not particular devices. Applicant respectfully submits that the mere discussion of an unauthorized person or pirate does not disclose or suggest preventing the computing device from modifying the set of filters as recited in amended claim 39.

For at least these reasons, Applicant respectfully submits that amended claim 39 is allowable over Jain in view of Boden.

With respect to claim 44, given that claim 44 depends from amended claim 39, Applicant respectfully submits that claim 44 is likewise allowable over Jain in view of Boden for at least the reasons discussed above with respect to amended claim 39.

With respect to amended claim 45, amended claim 45 recites:

> A network mediator comprising:
> a mapping of virtual addresses to network addresses;
> a set of filters that restrict the ability of the computing device to communicate with other computing devices; and
> a controller, coupled to the mapping, to,
> make a corresponding computing device aware of the virtual addresses,
> hide the network addresses from the computing device,
> receive, from the computing device, a data packet intended for a target computing device corresponding to a target virtual address,
> replace, based on the target virtual address, the target virtual address with the corresponding target network address,
> forward the data packet to the target computing device at the target network address,
> allow the set of filters to be modified from a remote device, and
> prevent the computing device from modifying the set of filters.

Applicant respectfully submits that no such network mediator is disclosed or suggested by Jain in view of Boden.

Jain, as discussed above, is directed to network devices for implementing virtual local area networks and virtual private networks. Boden, as discussed above, is directed to selective masquerading of internal IP addresses among a plurality of public IP address. However, nowhere in either Jain or Boden is there

any discussion or suggestion of a controller to allow the set of filters to be modified from a remote device and to prevent the computing device from modifying the set of filters as recited in amended claim 45.

Additionally, Applicant notes that in the rejection of claim 48 in the March 28, 2005 Office Action at ¶ 42, pp. 14-15, Audebert at col. 6, lines 46-61 and col. 12, lines 5-16 is cited as disclosing preventing unauthorized modification to filter software. These cited portions of Audebert discuss protecting filter software to prevent an unauthorized person reading and/or modifying the software, and preventing a pirate from using an integrated circuit card of a user without their knowledge. However, this prevention in Audebert is directed to particular persons, not particular devices. Applicant respectfully submits that the mere discussion of an unauthorized person or pirate does not disclose or suggest a controller to prevent the computing device from modifying the set of filters, but also to allow the set of filters to be modified from a remote device as recited in amended claim 45.

For at least these reasons, Applicant respectfully submits that amended claim 45 is allowable over Jain in view of Boden.

Claims 5, 6, 28-32, and 34-38 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of U.S. Patent No. 6,141,749 to Coss et al. (hereinafter "Coss") and further in view of U.S. Patent No. 6,466,932 to Dennis et al. (hereinafter "Dennis") or further in view of U.S. Patent No. 6,684,335 to Epstein, III et al. (hereinafter "Epstein"). Claim 5 has been canceled without prejudice, thereby rendering the rejection of claim 5. Applicant respectfully

submits that claims 6, 28-32, and 34-38 are not obvious over Jain in view of Coss and further in view of Dennis or Epstein.

With respect to Dennis, The subject application was filed October 24, 2000. Pursuant to 35 U.S.C. §103(c), which was amended effective Nov. 29, 1999 (Public Law 106-113),

> Subject matter developed by another person, which qualifies as prior art only under one or more of sub-sections (e), (f), and (g) of section 102 of this title, shall not preclude patentability under this section where the subject matter and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person.

Dennis issued on October 15, 2002 and was filed on March 16, 1999. The instant application was filed on October 24, 2000. Accordingly, Dennis would qualify as prior art only under the timing provisions of 35 U.S.C. §102(e). Both the subject application and Dennis were owned by, or subject to an obligation of assignment to, the same person or organization at the time the invention of the subject application was made. Given that the filing date of the subject application is after November 29, 1999, Applicant respectfully submits that Dennis is not a useable prior art reference under 35 U.S.C. §103(a) for the subject application.

With respect to Epstein, Epstein is directed to a resistance cell architecture (see, Title). As discussed in the Abstract of Epstein, each cell in the architecture comprises communication equipment such as a cell communication device coupled to one or more computers or terminals. Each cell is only permitted to communicate directly with certain predetermined other cells in the architecture. If a cell has a communication to be transmitted to a cell to which it does not directly

communicate, the communication will be sent from one cell to another until the communication reaches the intended recipient.

With respect to claim 6, claim 6 recites:

> A computing device as recited in 1, further comprising allowing the set of filters to be modified by a lower managerial level remote device only if the modifications are not less restrictive than modifications imposed by a higher managerial level remote device.

Applicant respectfully submits that no such allowing is disclosed or suggested by Jain in view of Coss and further in view of Epstein.

In the rejection of claim 6 in the March 28, 2005 Office Action at ¶ 13, p. 5, Epstein at col. 1, line 23 – col. 2, line 50, and col. 16, lines 27-41 is cited as disclosing the allowing of claim 6. Applicant respectfully disagrees. The cited portions of Epstein discuss that in the resistance cell architecture, "master" cells control many functions and the communication behavior of their subordinate cells (see, col. 2, lines 40-43). Also, in addition to being controlled by a master cell, each cell communication device can be programmed and controlled, to a limited extend, by a plurality of its own administrators and users (see, col. 16, lines 29-32). Various levels of administrators and users can be defined according to various security levels (see, col. 16, lines 32-34).

However, nowhere in the cited portions of Epstein is there any discussion or mention of allowing the set of filters to be modified by a lower managerial level remote device ***only if the modifications are not less restrictive than modifications imposed by a higher managerial level remote device.*** Although Epstein may mention that there may be various levels of administrators and users can be defined according to various security levels, the discussion of these different levels does not include any discussion or mention that a lower managerial level remote

device is allowed to modify a set of filters only if the modifications are not less restrictive than modifications imposed by a higher managerial level remote device. There is no discussion or mention in Epstein of determining whether modifications to a set of filters is to be allowed based on the restrictiveness of the modifications, much less of allowing the set of filters to be modified by a lower managerial level remote device only if the modifications are not less restrictive than modifications imposed by a higher managerial level remote device as recited in claim 6.

For at least these reasons, Applicant respectfully submits that claim 6 is allowable over Jain in view of Coss and further in view of Epstein.

With respect to claim 28, Applicant respectfully submits that, similar to the discussion above regarding claim 6, Jain in view of Coss and further in view of Epstein does not disclose or suggest allowing multiple remote computing devices, each corresponding to a different managerial level, to modify the set of filters, and preventing a lower managerial level device from modifying the set of filters in a manner that would result in a violation of a filter added by a higher managerial level device as recited in claim 28. For at least these reasons, Applicant respectfully submits that claim 28 is allowable over Jain in view of Coss and further in view of Epstein.

With respect to claim 29, claim 29 depends from claim 28 and Applicant respectfully submits that claim 29 is allowable over Jain in view of Coss and further in view of Epstein due to its dependency on claim 28. Furthermore, Applicant respectfully submits that Jain in view of Coss and further in view of Epstein does not disclose or suggest determining whether the request to modify

would result in a violation of a filter previously added to the set of filters by the higher managerial device as recited in claim 29.

In the March 28, 2005 Office Action at ¶ 14, pp. 5-6, Epstein at col. 1, line 23 – col. 2, line 50, and col. 16, lines 27-41 is cited as disclosing determining whether the request to modify would result in a violation of a filter previously added to the set of filters by the higher managerial device as recited in claim 29. Although Epstein may mention in these cited portions that there may be various levels of administrators and users can be defined according to various security levels, nowhere is there any discussion or mention of determining whether a request to modify the set of filters, received from a lower managerial level device, would result in a violation of a filter previously added to the set of filters by the higher managerial device as recited in claim 29. The mere mention of various security levels and various levels of administrators does not include any discussion or mention of such determining.

For at least these reasons, Applicant respectfully submits that claim 29 is allowable over Jain in view of Coss and further in view of Epstein.

With respect to claim 30, given that claim 30 depends from claim 29, Applicant respectfully submits that claim 30 is likewise allowable over Jain in view of Coss and further in view of Epstein for at least the reasons discussed above with respect to claim 29.

With respect to claims 31, 32, and 34, given that claims 31, 32, and 34 depend from claim 28, Applicant respectfully submits that claims 31, 32, and 34 are likewise allowable over Jain in view of Coss and further in view of Epstein for at least the reasons discussed above with respect to claim 28.

With respect to claim 35, Applicant respectfully submits that, similar to the discussion above regarding claim 6, Jain in view of Coss and further in view of Epstein does not disclose or suggest allowing a first computing device operating at a first of the multiple levels to modify a set of filters corresponding to a filtered device, and allowing a second computing device operating at a second of the multiple levels to modify the set of filters only if the modification is at least as restrictive as the filters imposed by the first computing device as recited in claim 35. For at least these reasons, Applicant respectfully submits that claim 35 is allowable over Jain in view of Coss and further in view of Epstein.

With respect to claims 36-38, given that claims 36-38 depend from claim 35, Applicant respectfully submits that claims 36-38 are likewise allowable over Jain in view of Coss and further in view of Epstein for at least the reasons discussed above with respect to claim 35.

Claims 7, 9, 19, 20, and 21-24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and further in view of Audebert. Applicant respectfully submits that claims 7, 9, 19, 20, and 21-24 are not obvious over Jain in view of Coss and further in view of Audebert.

With respect to claim 7, claim 7 recites:

> A method comprising:
> maintaining, at a computing device, a set of filters that restrict the ability of the computing device to communicate with other computing devices;
> allowing the set of filters to be modified from a remote device; and
> preventing the computing device from modifying the set of filters.

Applicant respectfully submits that no such method is disclosed by Jain in view of Coss and further in view of Audebert.

In the March 28, 2005 Office Action at ¶ 19, p. 7, Audebert at col. 6, lines 46-61 and col. 12, lines 5-16 is cited as disclosing preventing unauthorized modification to the filter program.

Col. 6, lines 46-61 of Audebert read as follows:

> at least one reprogrammable memory for storing at least one filter program translating said high-level requests into at least one of either (i) a sequence of at least one elementary command for being executed by said second software means of said second data processing means, or (ii) a sequence of data exchanges between said terminal module and said user via said second interface means, said data exchanges being executed by said first software means of said first data processing means, and
> means for protecting said filter software to prevent an unauthorised person reading and/or modifying said software, and

Col. 12, lines 5-16 of Audebert read as follows:

> The object of the invention is to prevent a pirate from using the integrated circuit card of a user without their knowledge, for example by modifying the filter software controlling the card or application software, or by loading a virus to bypass the application or the filter software. The embodiment described previously and its variants address these risks, by enabling verification of:
> the integrity of the filter software, and
> the source and the integrity of commands sent to the card via the reader 6, by authenticating them using a MAC, for example. The MAC can be verified by the reader 6 or the card 31. Equivalent protection could be obtained . . .

These cited portions of Audebert discuss protecting filter software to prevent an unauthorized person reading and/or modifying the software, and preventing a pirate from using an integrated circuit card of a user without their knowledge. However, there is no discussion or mention that this unauthorized

person or pirate is the computing device at which the set of filters is maintained, but that this unauthorized person or pirate is not a remote device. Furthermore, this prevention in Audebert is directed to particular persons, not particular devices. Applicant respectfully submits that the mere discussion of an unauthorized person or pirate does not disclose or suggest preventing the computing device at which the set of filters is maintained from modifying the set of filters as recited in claim 7.

For at least these reasons, Applicant respectfully submits that claim 7 is allowable over Jain in view of Coss and further in view of Audebert.

With respect to claims 9 and 19, given that claims 9 and 19 depend from claim 7, Applicant respectfully submits that claims 9 and 19 are likewise allowable over Jain in view of Coss and further in view of Audebert for at least the reasons discussed above with respect to claim 7.

With respect to claim 20, Applicant respectfully submits that, similar to the discussion above regarding claim 7, Audebert does not disclose or suggest a controller to prevent the computing device from modifying any of the filters in the set of filters as recited in claim 20. For at least these reasons, Applicant respectfully submits that claim 20 is allowable over Jain in view of Coss and further in view of Audebert.

With respect to claims 21, 23, and 24 given that claims 21, 23, and 24 depend from claim 20, Applicant respectfully submits that claims 21, 23, and 24 are likewise allowable over Jain in view of Coss and further in view of Audebert for at least the reasons discussed above with respect to claim 20.

With respect to claim 22, claim 22 depends from claim 20 and Applicant respectfully submits that claim 22 is allowable over Jain in view of Coss and further in view of Audebert due to its dependency on claim 20. Furthermore, Applicant respectfully submits that Jain in view of Coss and further in view of Audebert does not disclose or suggest a plurality of remote devices operating at a plurality of different managerial levels as recited in claim 22.

In the March 28, 2005 Office Action at ¶ 20, p. 7, it appears that Coss at col. 2, lines 30-43 is cited as disclosing a plurality of remote devices operating at a plurality of different managerial levels as recited in claim 22. However, the cited portion of Coss discusses dynamic rules that allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded. There is no discussion or mention in this cited portion of Coss of a plurality of different managerial levels, much less of a plurality of remote devices operating at a plurality of different managerial levels as recited in claim 22.

Jain and Audebert are not cited as curing, and do not cure, these deficiencies of Coss. For at least these reasons, Applicant respectfully submits that claim 22 is allowable over Jain in view of Coss and further in view of Audebert.

Claims 8 and 17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and further in view of Audebert and further in view of U.S. Patent No. 6,266,707 to Boden et al. (hereinafter "Boden2"). Applicant respectfully submits that claims 8 and 17 are not obvious over Jain in view of Coss and further in view of Audebert and further in view of Boden2.

Boden2 is directed to firewall capability for a gateway system, and IP network address translation (NAT) and IP filtering with dynamic address resolution (see, col. 1, lines 20-23). As discussed in the Abstract of Boden2, symbolic interface names are recognized in selected rule statements. A symbolic s-rule file is generated from these rule statements which includes symbolic interface names. During processing of a packet message, the s-rule file corresponding to the interface name in the packet message is processed, with symbolic addresses in the s-rule file resolved to the IP addresses obtained from the packet message.

With respect to claims 8 and 17, claims 8 and 17 depend from claim 7 and Applicant respectfully submits that claims 8 and 17 are allowable over Jain in view of Coss and further in view of Audebert for at least the reasons discussed above with respect to claim 7. Boden2 is not cited as curing, and does not cure, the deficiencies of Jain, Coss, and Audebert discussed above with respect to claim 7. Accordingly, for at least these reasons, Applicant respectfully submits that claims 8 and 17 are allowable over Jain in view of Coss and further in view of Audebert and further in view of Boden2.

Claims 10-14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and further in view of Audebert and further in view of U.S. Patent No. 6,510,154 to Mayes et al. (hereinafter "Mayes"). Applicant respectfully submits that claims 10-14 are not obvious over Jain in view of Coss and further in view of Audebert and further in view of Mayes.

Mayes is directed to a security system for network address translation systems (see, Title). As discussed in the Abstract of Mayes, a system and method

are provided for translating local IP addresses to globally unique IP addresses. This allows local hosts in an enterprise network to share global IP addresses from a limited pool of such addresses available to the enterprise. The translation is accomplished by replacing the source address in headers on packets destined for the Internet and by replacing destination address in headers on packets entering the local enterprise network from the Internet. Packets arriving from the Internet are screened by an adaptive security algorithm. According to this algorithm, packets are dropped and logged unless they are deemed nonthreatening. DNS packets and certain types of ICMP packets are allowed to enter local network. In addition, FTP data packets are allowed to enter the local network, but only after it has been established that their destination on the local network initiated an FTP session.

With respect to claims 10-14, claims 10-14 depend from claim 7 and Applicant respectfully submits that claims 10-14 are allowable over Jain in view of Coss and further in view of Audebert for at least the reasons discussed above with respect to claim 7. Mayes is not cited as curing, and does not cure, the deficiencies of Jain, Coss, and Audebert discussed above with respect to claim 7. Accordingly, for at least these reasons, Applicant respectfully submits that claims 10-14 are allowable over Jain in view of Coss and further in view of Audebert and further in view of Mayes.

Furthermore, with respect to claim 10, in the March 28, 2005 Office Action at ¶ 27, pp. 9-10, Mayes at the abstract and col. 1, line 9 – col. 2, line 32 is cited as disclosing wherein one or more filters in the set of filters restrict one or more of the transmission of data packets of a particular type from the computing device and reception of data packets of a particular type at the computing device as

recited in claim 10. Furthermore, in the March 28, 2005 Office Action at ¶ 56, p. 20, it was asserted that claim 10 does not emphasize the limitation of bi-directional communication.

Applicant respectfully submits that the cited portions of Mayes discuss a security algorithm to keep unwanted packets from external sources out of a private network (see, col. 2, lines 19-22). According to the security algorithm, packets arriving from the internet are screened, and are dropped and logged unless they are deemed nonthreatening (see, Abstract). Thus, Mayes discusses screening *received* packets, not packets to be transmitted. In contrast, in claim 10 one or more filters restrict one or more of the *transmission* of data packets of a particular type from the computing device and *reception* of data packets of a particular type at the computing device. As transmitted and received data packets are both recited in claim 10, Applicant respectfully submits that claim 10 does cover bi-directional communication. Mayes, on the other hand, is directed to screening uni-directional communication – Mayes discusses screening packets that are received from the internet, not packets transmitted to the internet. This uni-directional screening is explicitly acknowledged later in Mayes, which states that "there is essentially no security mechanism to block outbound packets" (see, col. 7, lines 13-15). Applicant respectfully submits that the discussion of screening packets arriving from the internet does not disclose or suggest wherein one or more filters in the set of filters restrict one or more of the transmission of data packets of a particular type from the computing device and reception of data packets of a particular type at the computing device as recited in claim 10.

For at least these reasons, Applicant respectfully submits that claim 10 is allowable over Jain in view of Coss and further in view of Audebert and further in view of Mayes.

Claims 15 and 16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and further in view of Audebert and further in view of Dennis or Epstein. Applicant respectfully submits that claims 15 and 16 are not obvious over Jain in view of Coss and further in view of Audebert and further in view of Dennis or Epstein.

As discussed above with respect to Dennis, Applicant respectfully submits that Dennis is not a useable prior art reference under 35 U.S.C. §103(a) for the subject application

With respect to claim 15, claim 15 depends from claim 7 and Applicant respectfully submits that claim 15 is allowable over Jain in view of Coss and further in view of Audebert for at least the reasons discussed above with respect to claim 7. Epstein is not cited as curing, and does not cure, the deficiencies of Jain, Coss, and Audebert discussed above with respect to claim 7. Accordingly, for at least these reasons, Applicant respectfully submits that claim 15 is allowable over Jain in view of Coss and further in view of Audebert and further in view of Dennis or Epstein.

With respect to claim 16, claim 16 depends from claim 7 and Applicant respectfully submits that claim 16 is allowable over Jain in view of Coss and further in view of Audebert for at least the reasons discussed above with respect to claim 7. Epstein is not cited as curing, and does not cure, the deficiencies of Jain, Coss, and Audebert discussed above with respect to claim 7.

Furthermore, in the March 28, 2005 Office Action at ¶ 34, p. 12, Epstein at col. 1, line 23 – col. 2, line 50, and col. 16, lines 27-41 is cited as disclosing allowing the set of filters to be modified by a lower managerial level remote device only if the modifications are not less restrictive than modifications imposed by a higher managerial level remote device as recited in claim 16. Applicant respectfully submits that, similar to the discussion above regarding claim 6, Epstein does not disclose or suggest allowing the set of filters to be modified by a lower managerial level remote device only if the modifications are not less restrictive than modifications imposed by a higher managerial level remote device as recited in claim 16.

For at least these reasons, Applicant respectfully submits that claim 16 is allowable over Jain in view of Coss and further in view of Audebert and further in view of Dennis or Epstein.

Claims 18 and 25-27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and further in view of Audebert and further in view of U.S. Patent No. 6,510,509 to Chopra et al. (hereinafter "Chopra"). Applicant respectfully submits that claims 18 and 25-27 are not obvious over Jain in view of Coss and further in view of Audebert and further in view of Chopra.

Chopra is directed to methods and apparatus for network gateway devices that implement firewall, IP routing, quality of service, load balancing, and/or network address translation rules (see, col. 1, lines 7-10). As discussed in the Abstract of Chopra, a high-speed rule processing apparatus is disclosed that may be used to implement a wide variety of rule processing tasks such as network address translation, firewall protection, quality of service, IP routing, and/or load

balancing. The high-speed rule processor uses an array of compare engines that operate in parallel.

With respect to claim 18, claim 18 depends from claim 7 and Applicant respectfully submits that claim 18 is allowable over Jain in view of Coss and further in view of Audebert for at least the reasons discussed above with respect to claim 7. Chopra is not cited as curing, and does not cure, the deficiencies of Jain, Coss, and Audebert discussed above with respect to claim 7.

Furthermore, in the March 28, 2005 Office Action at ¶ 36, p. 12, it was asserted that "It is well known in the art to filter packets according to mask values." Applicant respectfully disagrees. None of Jain, Coss, Audebert, and Chopra disclose, or are cited as disclosing, wherein each filter parameter includes a filter value and a mask value indicating which portions of the filter value must match a corresponding parameter in a data packet for the data packet to satisfy the filter as recited in claim 18. If this rejection is maintained, Applicant respectfully requests that a reference teaching this element of claim 18 be cited.

For at least these reasons, Applicant respectfully submits that claim 18 is allowable over Jain in view of Coss and further in view of Audebert and further in view of Chopra.

With respect to claim 25, claim 25 depends from claim 20 and Applicant respectfully submits that claim 25 is allowable over Jain in view of Coss and further in view of Audebert for at least the reasons discussed above with respect to claim 20. Chopra is not cited as curing, and does not cure, the deficiencies of Jain, Coss, and Audebert discussed above with respect to claim 20. Furthermore, similar to the discussion above regarding claim 18, Applicant respectfully submits

that the cited references do not disclose or suggest wherein each filter parameter includes a filter value and a mask value indicating which portions of the filter value must match a corresponding parameter in the data packet for the data packet to satisfy the filter as recited in claim 25. For at least these reasons, Applicant respectfully submits that claim 25 is allowable over Jain in view of Coss and further in view of Audebert and further in view of Chopra.

With respect to claims 26 and 27, given that claims 26 and 27 depend from claim 25, Applicant respectfully submits that claims 26 and 27 are likewise allowable over Jain in view of Coss and further in view of Audebert and further in view of Chopra for at least the reasons discussed above with respect to claim 25.

Claim 33 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Coss and further in view of Audebert and further in view of Dennis or Epstein and further in view of Chopra. Applicant respectfully submits that claim 33 is not obvious over Jain in view of Coss and further in view of Audebert and further in view of Dennis or Epstein and further in view of Chopra.

As discussed above with respect to Dennis, Applicant respectfully submits that Dennis is not a useable prior art reference under 35 U.S.C. §103(a) for the subject application.

Claim 33 depends from claim 28 and Applicant respectfully submits that claim 33 is allowable over Jain in view of Coss and further in view of Epstein for at least the reasons discussed above with respect to claim 28. Audebert and Chopra are not cited as curing, and do not cure, the deficiencies of Jain, Coss, and Epstein discussed above with respect to claim 28. Furthermore, similar to the discussion above regarding claim 18, Applicant respectfully submits that the cited

references do not disclose or suggest wherein each filter parameter includes a filter value and a mask value indicating which portions of the filter value must match a corresponding parameter in a data packet for the data packet to satisfy the filter as recited in claim 33. For at least these reasons, Applicant respectfully submits that claim 33 is allowable over Jain in view of Coss and further in view of Audebert and further in view of Epstein and further in view of Chopra.

Claims 40 and 41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden and further in view of U.S. Patent No. 6,728,885 to Taylor et al. (hereinafter "Taylor"). Applicant respectfully submits that claims 40 and 41 are not obvious over Jain in view of Boden and further in view of Taylor.

Taylor is directed to firewall technology in packet switched networks for adaptively providing a plurality of security levels (see, col. 1, lines 12-14). As discussed in the Abstract of Taylor, the method comprises the step of receiving a first communication packet on at least one network interface port from an outside network, and further includes the steps of filtering the first packet in one of at least two levels of security comprising a first level of security which examines the content information of the packet and a second level of security which examines the first packet excluding the content information of the packet.

With respect to claims 40 and 41, claims 40 and 41 depend from claim 39 and Applicant respectfully submits that claims 40 and 41 are allowable over Jain in view of Boden for at least the reasons discussed above with respect to claim 39. Taylor is not cited as curing, and does not cure, the deficiencies of Jain and Boden discussed above with respect to claim 39. For at least these reasons, Applicant

respectfully submits that claims 40 and 41 are allowable over Jain in view of Boden and further in view of Taylor.

Claims 42 and 48 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden and further in view of Coss and further in view of Audebert. Claims 42 and 48 have been canceled without prejudice, thereby rendering the rejection of claims 42 and 48 moot.

Claim 43 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden and further in view of Coss and further in view of Dennis or Epstein. Applicant respectfully submits that claim 43 is not obvious over Jain in view of Boden and further in view of Coss and further in view of Dennis or Epstein.

As discussed above with respect to Dennis, Applicant respectfully submits that Dennis is not a useable prior art reference under 35 U.S.C. §103(a) for the subject application.

Claim 43 depends from claim 39 and Applicant respectfully submits that claim 43 is allowable over Jain in view of Boden for at least the reasons discussed above with respect to claim 39. Coss and Epstein are not cited as curing, and do not cure, the deficiencies of Jain and Boden discussed above with respect to claim 39.

Furthermore, in the March 28, 2005 Office Action at ¶ 45, p. 15, Epstein at col. 1, line 23 – col. 2, line 50, and col. 16, lines 27-41 is cited as disclosing preventing a lower managerial level device from modifying the set of filters in a manner that would result in a violation of a filter added by a higher managerial level device as recited in claim 43. Applicant respectfully submits that, similar to

the discussion above regarding claim 6, Epstein does not disclose or suggest preventing a lower managerial level device from modifying the set of filters in a manner that would result in a violation of a filter added by a higher managerial level device as recited in claim 43.

For at least these reasons, Applicant respectfully submits that claim 43 is allowable over Jain in view of Boden and further in view of Coss and further in view of Dennis or Epstein.

Claims 46 and 47 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Jain in view of Boden and further in view of Audebert. Applicant respectfully submits that claims 46 and 47 are not obvious over Jain in view of Boden and further in view of Audebert.

Claims 46 and 47 depend from claim 39 and Applicant respectfully submits that claims 46 and 47 are allowable over Jain in view of Boden for at least the reasons discussed above with respect to claim 39. Audebert is not cited as curing, and does not cure, the deficiencies of Jain and Boden discussed above with respect to claim 39. For at least these reasons, Applicant respectfully submits that claims 46 and 47 are allowable over Jain in view of Boden and further in view of Audebert.

Furthermore, with respect to claim 47, claim 47 recites in part "wherein the computing device includes the network mediator". Applicant respectfully submits that there is no disclosure or suggestion in Jain, Boden, and/or Audebert of the computing device that the data packet is received from includes the network mediator as recited in claim 47.

Applicant notes that Audebert discusses protecting filter software to prevent an unauthorized person reading and/or modifying the software, and preventing a pirate from using an integrated circuit card of a user without their knowledge. However, there is no discussion or mention that this unauthorized person or pirate is the computing device that includes the network mediator comprising a mapping, a set of filters, and a controller as recited in claim 47, and that that computing device is prevented from modifying the set of filters, but that the set of filters is allowed to be modified by from a remote device. Without any such discussion or suggestion, Applicant respectfully submits that Audebert cannot disclose or suggest wherein the computing device includes the network mediator as recited in claim 47. For at least these reasons, Applicant respectfully submits that claim 47 us allowable over Jain in view of Boden and further in view of Audebert

Applicant respectfully requests that the §103 rejections be withdrawn.

Conclusion

Claims 1, 4, 6-41, and 43-47 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: 9/13/05

By: _____

Allan T. Sponseller
Reg. No. 38,318
(509) 324-9256